Department of Defense Explosives Safety Board (DDESB)
Performance Work Statement – AMD 1
21 Nov 18

1. Background

The Department of Defense Explosives Safety Board (DDESB), formerly called the Armed Forces Explosives Safety Board, was established in 1928 by the Seventieth Congress after a major disaster occurred at the Naval Ammunition Depot, Lake Denmark, New Jersey in 1926. The accident virtually destroyed the depot, causing heavy damage to adjacent Picatinny Arsenal and the surrounding communities, killing 21 people, and seriously injuring 53 others. The monetary loss to the Navy alone was $84 million. As a result of a full-scale Congressional investigation, Congress directed the establishment of the Board to provide oversight of the development, manufacture, testing, maintenance, demilitarization, handling, transportation and storage of explosives, including chemical agents on DoD facilities worldwide. The DDESB mission is to provide objective advice to the Secretary of Defense and all Service Secretaries on matters concerning explosives safety and to prevent hazardous conditions to life and property on and off Department of Defense installations from the explosives and environmental effects of DoD titled munitions.

The Defense Explosive Safety Knowledge Enterprise Services (DESKES) is a moderate sensitivity system generated from the DoD Explosives Safety Strategic Plan. One of the goals of this plan is to transform the DDESB to effectively support the DoD mission. Another goal is to develop and implement a Knowledge Management (KM) plan to optimize explosive safety management. The plan specifically details the four functional divisions that include: 1) Tools, 2) Collaborative Environments, 3) Technical Library and Historical Archives, and 4) Metrics. These functional divisions are the basis for the DESKES portal design and implementation.

DESKES supports DDESB mission execution, and planning which includes more effective support to the DoD mission. DESKES will have a Fthrpositive impact on the DDESB customer organization, since project processes and deliverables will help DDESB increase its KM capabilities, document business processes and workflow, capture metrics for use in reports and process improvement plans and increase collaborative work both within DDESB and with external Joint Military services stakeholders.

Department of Defense Explosives Safety Board (DDESB), 4800 Mark Center Dr, Alexandria, VA requires contractor support services for cloud application hosting, operations and maintenance and optional enhancements for the enterprise-wide DoD Explosives Safety Knowledge Enterprise System (DESKES), Joint Hazard Classification System (JHCS), and Explosives Safety Mishap Analysis Module (ESMAM) applications. These applications support the mission of DDESB by serving as the agency-wide records management of explosives data and safety, to prevent hazardous conditions to life and property on and off Department of Defense installations from the explosives and environmental effects of DoD titled munitions. This task order will provide support for the operational maintenance of the DESKES suite of applications including all necessary updates, corrective action of escaped defects or on behalf of user operations, security mitigation solutions and support of future-contracted enhancements. The support of this application will also include the incorporation and ongoing maintenance of workflows presently existing as well as those developed by enhancements. The Contractor shall use industry best practices and Federal guidelines for ensuring the optimal support of the

DESKES. As identified in code review, security audits, health checks or other reviews of the application, the Contractor shall identify a plan to incorporate changes to ensure the secure, stable and sustainable maintenance of the application in the DDESB environment. Where applicable the Contractor shall solicit feedback, clarification or suggest modifications to ordering or sequencing of events that will improve the business process. The application contributes to achieving the DDESB Strategic Objectives including increasing the efficiency of DDESB operations by providing tools to manage projects supporting completing new projects on schedule and delivering better value and savings by providing a tool to help improve data quality and reporting.

2. Scope of Work

The Contractor shall provide all personnel, administration, management and local travel necessary in support of the DESKES application suite and ensure its success by providing support in the following areas:

- Operation and Maintenance
- Program Management
- Tier I - III Helpdesk Services
- Software and Engineering Lifecycle Support
- Information Assurance and Cyber Security Support
- Optional Enhancement Support

This work will include but is not limited to cloud hosting services, software development, integration, testing, maintenance, audit support, system analysis, impact analysis, documentation, reports, and progress monitoring using reporting procedures and measures of performance. These shall be in accordance with industry best practices, NIST, OMB and guidance.

Should DDESB choose to move towards a more Agile methodology, the Contractor, when possible, shall execute processes in a sustainable and repeatable process using an Agile methodology of identifying, describing, testing and delivering technical solutions.

The Contractor shall be responsible for the integration and support of the application including all enhancements made to the application.

2.1. CORE Support – CLIN 1

The Contractor shall provide support for the application development, operation and maintenance, and performance monitoring of the DESKES application suite for all environments which includes production, pre-production, development, and testing. The Contractor shall coordinate all technical implementation tasks with Government-designated support teams including server, application, network and/or security teams. This task includes the technical support, changes and architectural expertise to maintain the application in compliance with all existing Army/DISA policies and guidelines. Issues that may be discovered through scan, reviews, audits throughout the task and phase-out periods shall be resolved in the timeframes defined by DISA Policy. The Contractor shall meet and comply with all DoD IT Security

Policies and all applicable NIST standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.

2.1.1. Operation and Maintenance

2.1.1.1 Operations

The Contractor shall ensure the DESKES application suite is operational and fully functional with no performance or access degradation at the end of the phase-in period.

- Identifying and repairing defects resulting from design errors, logic errors and coding errors.
- The Contractor shall document the defects resulting from: data processing errors, system performance errors, escaped defects from internal quality control (IV&V) and user acceptance testing (UAT), or reported through a help desk or other incident identification methods.

The Contractor shall:

○ Ensure the application is operable using the DoD list of approved desktop and server software.

○ Ensure the application remains optimally operational following industry best practices of design and technical operating environments. The Contractor shall recommend technical configurations that may improve performance, availability or stability. The Contractor shall ensure the application is optimally available given the architecture, toolsets, configurations and resources available within the agency.

○ Notify the Government of hotfixes or end-of-life dates to the operating system, middleware, database or supporting technical platforms (including patches) impacting the usability or having an impact on the application. Contractor shall be responsible for coordinating with the government to ensure components of the application will be upgraded prior to the end-of-life hardware/software.

○ Ensure the application remains operable following changes to the environment where the application sits. The application will optimally perform with these patches in accordance to IT Security Policy and prior to Government-designated published update cycles. The environment change may result from a change in business rules or processes, government policies, and software and hardware platforms. This is not meant to state that the Vendor is responsible for making the environmental changes under O&M; however, the nature of ensuring the application remains operable after environmental changes may necessitate changes to the application for it to remain operable. Such changes covered under O&M may include configuration changes to the application, links, Web Service Description Language (WSDL), APIs, and pointers including verification of these changes should apply. Functionality resulting from new business rules, processes or procedures will necessitate a developmental enhancement. Changes to address new features (those parts, pieces, components, workflows, procedures, integrations or connections) that do not presently exist, are not within the scope of O&M.

The Contractor shall support server or data migrations to ensure applications are operational post-migration. Migration activities may include any environment, on-prem server to server, data conversions, on-prem to cloud, cloud to cloud, cloud to on-prem application refactoring or other.

The Contractor shall perform maintenance to ensure the application meets minimum accepted performance targets. Maintaining the system's performance, maintainability, reliability and security shall follow emerging standards such as the Consortium for IT Software Quality (CISQ) (http://it-cisq.org/standards/), including the updating of documentation and the upgrade of components, frameworks, versions to maintain the technical operation of the information system. The Contractor shall ensure the corrective response is within the minimally recommended date. Current policy requires all high and critical findings, as defined by the DoD Scanning Tool, to be resolved within 30 days.

Root Cause Analysis (RCA). As part of daily operations, any outage must be reported, this includes any escape defect, logic error and/or coding errors. For any outage, the Contractor shall initiate a RCA.

The RCA prepared by the Contractor shall indicate the error, its symptoms and the impact of the error on present operations. If a workaround is available this shall be documented as well as any other instructions for end users or Tier 1 helpdesk personnel to use until the error is corrected.

The report shall indicate the time the defect was first reported as well as progress notes (including resolution estimates if known). This report shall explain in non-technical language all pertinent details of the error and resolution once the error's solution is known.

The initial report shall be delivered via email to the Government Program Manager and COR. Each report shall indicate the next estimated update. The Contractor shall make updates to the PM and COR following this schedule and/or when requested by the Government.

The Contractor shall deliver services to include product configuration and solutioning expertise sufficient to evaluate change requests, propose optimal solutions, coordinate, and execute change related activities across the entire DESKES suite.

2.1.1.2 Maintenance

The Contractor shall maintain all current application interfaces with other applications, as well as any application interfaces established in the future. Contractor shall support other Contractors supporting an interfacing application with activities to include, but not be limited to troubleshooting interface issues. Vendor shall work with any vendor at the Government's request to support activities by the other vendor to establish a new interface with DESKES. The intent is not for the Vendor to establish the interface, but rather to participate in the discussions and planning for the new interface. An "interface" is any connection between applications for purposes of exchanging information.

The Contractor shall provide support on specified IT assets to include Windows and non-Windows (Unix) virtual and stand-alone operating systems, monitoring, and Commercial Off the Shelf (COTS) applications. The contractor shall:

1. Perform system deployment and adherence to AWS GovCloud and industry standard deployment method.

2. Apply patches, manage file systems, monitor performance and troubleshoot alerts from contractor-provided monitoring tools.
3. Perform system failure analysis and recovery; ensuring the consistency and integrity of file systems.
4. Perform system security patching, upgrades, and configuration/policy changes in compliance with all relevant and required Information Assurance (IA) and security implementation/compliance requirements, including DISA Security Technical Information Guides (STIGs), identified during STIG reviews, Gold Disk, vulnerability Scans, etc.
5. Administer accounts user access control to the systems that the contractor administers.
6. Monitor the system logs for growth patterns, trends, and intrusion detection.
7. Provide test support to include supporting integration testing, analyzing test results and assisting in acceptance testing of software components.
8. Conduct research and investigation into technological developments in such areas as operating systems, and software systems for installing, monitoring and maintaining operating systems and executive software.
9. Install, configure and maintain COTS/GOTS software products that provide operating system support such as HBSS, ACAS and other products per DDEBS direction.
10. Configure and maintain system backups to conform to IA controls requirements.
11. Assist with the research and supporting analysis, and design of virtual server specifications and configurations that will feed into a Government decision.
12. Maintain the integrity of system baselines and provide audit checks of all systems and backups as required.
13. Perform system/application diagnostics through the use of Government-provided maintenance tools to ensure availability and to provide a notification vehicle of problems to administrators.
14. Maintain control and documentation. The contractor shall assist the Government in maintaining configuration control of source code and related technical documents within the protected development environment and within the Development Enclave.

2.1.2. Program Management

The contractor shall provide program management support throughout the task order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the task/subtasks identified in this task order.

The contractor shall designate a Program Manager (PM) by name for all programmatic issues, concerns or updates. The PM shall be responsible for overall execution of this task and shall have full authority to make decisions and commit the contractor's organization under this task. The Contractor PM shall respond to DDESB's questions, concerns, and comments. The Contractor PM shall be proactive in alerting DDESB to potential contractual issues including situations that may compromise the contractor's ability to provide the required services.

2.1.2.1. Prepare a Monthly Status Report (MSR)

The contractor shall develop and provide an MSR using Microsoft (MS) Office Suite applications, by the 10th calendar day of each month via electronic mail to the PM and the COR. The MSR shall include, but is not limited to, the following:

1. Activities during reporting period, by task and subtask to include (but not limited to) on-going activities, new activities, activities completed; progress to date on all above-mentioned activities. Each section shall begin with a brief description of the task.
2. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
3. Personnel gains, losses, and status (to include DoD clearance, badging status, security clearance, etc.).
4. Government actions required.
5. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
6. Information pertaining to the execution of the task as requested by the Government Program Manager or Contract Officer Representative.
7. Summary of any enhancement activities performed under Section 3.2, if applicable.
8. Summary of Help Desk ticket history for activities performed to include (but not limited to) tickets opened and closed, metrics on the number of referrals during the month as well as cumulative requests, the user's region, the types of requests, time to respond to requests, time to resolve requests, and number of unresolved referrals. The metrics shall be submitted as part of the monthly report.

2.1.2.2. Provide Program Documentation Management

The contractor shall create and maintain files that document the processing of work products, deliverables and other associated information pertaining to actions performed under this task. The contractor shall maintain within the Government-designated electronic repositories. Examples of files include, but not limited to, the following:

1. Documentation providing traceability and rationale for the contractor's technical program decisions.
2. The latest internally controlled version of all specifications, drawings, databases, and software that define or implement the system.
3. Detailed Standard Operating Procedures (SOPs)
4. All configuration management documentation.
5. SOW work products and deliverables.
6. Updates related to reporting artifacts (including and not limited to data dictionary changes impacts from enhancements) to reporting team and downstream data consumers.

The contractor shall provide the government access to all records to ensure mission support is not interrupted. Upon completion of the task, the Contractor shall turn over all such records to DDESB in approved formats.

2.1.2.3. Application Technical Roadmap

The Contractor shall deliver an application technical roadmap for the application. This document shall include the components the application is required to run (including Operating System, Database, Middleware, Technical Platforms (if any) and ancillary supporting application, modules, or software packages. For each component a transition plan including retirement dates for support shall be included when known.

This technical roadmap shall document the recommended timeframe to ensure all system components remain supported within standard support schedules (i.e. support shall remain within the standard support period).

2.1.3. Defect Resolution

The Contractor shall:

- For any identified defects in the O&M system(s) that the Contractor must fix, the Contractor shall report the following to DDESB weekly:
    - Defects – Total number of software defects, by assigned severity category, recorded during the following phases:
        - Defects found from start of formal system testing phase, up to release of software;
        - Defects found during piloting;
        - Defects found from start of deployment to end customer, through first three months of operational use after deployment; and
        - Defects found during operations and maintenance.
    - Provide status reports of defect resolutions

2.1.4. Tier I-III Helpdesk Services

The Contractor shall provide Tier I, II, and III Customer Support Services for the DESKES application and infrastructure. The Contractor will be responsible for logging of trouble tickets, user inquiries, enhancements, and database change requests. At DDESB discretion, DDESB can require the Contractor to log these items into a DDESB hosted ticketing system.

A designated O&M DESKES Team support email group shall be established and maintained by the Contractor. Tier I and III tickets requiring resolution support from the Contractor will be escalated to different tiers. The help desk shall assist in troubleshooting application specific issues and supporting ad-hoc urgent requests.

The Contractor shall keep metrics shall on the number of referrals during the month as well as cumulative requests, the user's region, the types of requests, time to respond to requests, time to resolve requests, and number of unresolved referrals. The metrics shall be submitted as part of the monthly report.

Helpdesk support tiers are defined as:

- Tier I: DDESB will provide simple local and phone support. At this level, the customer may possess a broad understanding of DESKES and may not understand the inner workings. In this case, the specialist would identify a customer's needs and provide tips on how to manage a problem. Typically, these solutions are in a FAQ or knowledge base. Also, log-in issues are resolved here. When a tier-1 support team member is not able to resolve the issue, they classify the problem and pass it on to the appropriate tier-2 specialist.
- Tier II: involves technical knowledge and is staffed by technicians who have troubleshooting capabilities beyond the tier-1 support. If the issue is an existing one, the tier-II specialist will research a solution or a workaround. In cases where there is no solution, it should be logged as an open bug. If a customer experiences a new issue, further analysis has to be done to see if it can be resolved. If the tech cannot fix the problem at this tier, the problem goes to tier-III.
- Tier III: This tier engages the technical expertise of those involved in development. This is where the complex issues and any outstanding that were escalated in the previous tiers are addressed. Usually, the work performed at this tier results in a system release

2.1.5. Software and Engineering Lifecycle Support

All DESKES application development will be executed to match the agile development life cycle in order to deliver capability more rapidly and in closer alignment with defined requirements. To accomplish this task, the contractor shall accomplish the following:

1. Requirements management. The contractor shall establish and maintain a requirements management process based on industry standards and best practices.

2. Software support management. The contractor shall establish and maintain an agile software development management process using SCRUM methods.

3. Software project management. The contractor shall establish and maintain an agile project management process based on best practices and focuses on managing incremental deliveries within an established schedule.

4. Development Iterations and Continuous Integration. The contractor shall establish and follow agile development processes using short duration development cycles or "sprints" that produce demonstrable "interim deliveries" of software and using continuous integration best practices in developing software capabilities. The length of sprints will be determined by the release plan and are anticipated to be 1-2 weeks in duration but not exceeding 3 weeks.

5. Release Planning. The contractor shall participate in the release planning process with other Government directed representatives. Release planning and final determination of

release content is the responsibility of the Government, but the contractor shall provide knowledge and input that is deemed critical by the Government to the planning process.

6. Secure Software Design. The contractor shall establish processes and procedures to ensure and demonstrate that developed applications are devoid of security flaws.

7. Testing. The contractor shall deliver a test plan describing how it will conduct and measure testing progress (e.g. unit, functional, nonfunctional, system, interoperability, regression, security, performance, usability, reliability, supportability) of software throughout the development lifecycle using continuous integration methods and automated regression testing utilities.

2.1.5.1. DDESB Operational Software Specific Support Services

The contractor shall provide administration, and testing expertise to government/contractor agile teams to improve features, functionality, and integration of artifacts, data models, services, system specifications and architectures. JHCS/ESMAM Integration, DESKES/SSMM Functionality Improvements, and Capabilities listed below, will be prioritized and directed by the DDESB Program Office.

2.1.5.2. Joint Hazard Classification System (JHCS)

The Contractor shall provide the following development support: Upgraded Integrated User Experience; Improved functionality and automation; expanded records and reporting capabilities; improved content management and storage capability; synchronization of Group items; expanded field capability; and expanded document tracking, subject to Government representative prioritization.

2.1.5.3. Explosives Safety Mishap Analysis Module (ESMAM)

The Contractor shall provide the following development support: Expanded records and reporting capabilities; and expanded storage capability, subject to Government representative prioritization.

2.1.5.4. DESKES

The Contractor shall provide the following development support: Modification of the DESKES GUI Interface; and Improving Tasker Tracking capabilities, subject to Government representative prioritization.

2.1.5.5. Safety Submission Management Module (SSMM)

The Contractor shall provide the following development support: Upgrading the Integrated User Experience; functionality and automation requirements; and improved Search Function capabilities, subject to Government representative prioritization.

2.1.5.6. Subject Matter Expertise (SME) Support

The contractor shall support the government with Subject Matter Experts (SMEs) proficient in the software architectures, engineering, and integration. The offer shall assign a SME to support

the government with application development expertise required for briefings, conferences, technology or capability demonstrations, and Program Reviews. SME support is also required for handling issues or tickets escalated from Operations, Tier III, or DDESB Management to resolve production problems and/or to provide recommended courses of action.

The contractor shall have available sufficient and qualified SMEs that have proficiency and familiarity with COBRA 2000 Web Service Architecture, Army/DISA IA processes, and AWS GovCloud industry best practices with supporting operational systems, services and capabilities including the considerations required for service interruptions and smooth rollout of new capabilities or upgrades, the troubleshooting methods to employ in the event of a service or capability outage or incident, supporting failover and disaster recovery of services and capabilities, and ensuring proper maintenance coverage and identifying capabilities nearing end of life or support.

The offer shall propose a sufficient number of SMEs with proficiency in each area, contractor shall provide at least one SME cleared to SECRET level to provide support to DDESB.

2.1.6. Information Assurance and Cyber Security Support

The contractor shall provide information system security expertise for both operational and test environment implementation of security configurations. This task will provide for IA and Certification and Accreditation (C&A)/Risk Management Framework (RMF) (collectively referred to as IA) necessary to ensure that the network is not breached or disrupted by malicious or unintentional actions. IA tasks at a minimum shall include the following subtasks:

The contractor shall create and maintain the plan of action and milestones (POA&M) to detail actions necessary to maintain and renew the Authority to Operate (ATO) granted by the designated Authorizing Official (AO).

The contractor shall identify system vulnerabilities and develop mitigation plans to resolve vulnerability issues as required. The Contractor shall deliver corrective responses to security findings ensuring compliance with Government security requirements. Delivery of these corrective security findings shall be conducted within the timeline designated by audit teams, or may follow prescribed deadlines.

The contractor shall create appropriate documentation for the ATO accreditation decision as well as the results of the implementation of required baseline security and additional controls that may be required by the DoD component or local IAM.

The contractor shall perform baseline and validation IA vulnerability scans to determine the risk to the DESKES hardware and software baselines. Testing shall include automated tools, manual STIG checklist and interviews of key personnel.

The Contractor shall provide information systems engineering analysis and support for the purpose of testing, evaluating and integrating Cybersecurity/IA products and tools that provide

the DDESB's Cybersecurity/IA Defense in Depth capability and Threat analysis. The Contractor shall coordinate the assessment and acquisition of Cybersecurity and IA tools with DoD to support DDESB Cybersecurity initiatives. The support shall include:

- Assessing/ Improve the security posture of select information systems networks, and technologies.
- Recommending information systems and network security solutions that support the Army Cybersecurity/IA program and identify new, state-of-art enabling technologies communications, and computers (C4) architecture.
- Conducting process reviews and proposing recommendations for process improvement to Cybersecurity/IA programs.

2.2 Optional Labor Support Ceiling – CLIN 2

The contractor shall include the required provisions for Optional support, as defined below, throughout the task order life cycle per the Fair Opportunity Notice (FON) instructions, which includes the requirement for a lump sum CLIN 0002 Optional Labor allotment for Optional Labor support. It is anticipated that the workload will fluctuate, and surge support may be required based on fluid schedule requirements; therefore, the support will be obtained via the utilization of the CLIN 0002 Optional Labor CLIN. Such support may encompass the entire scope of work identified in CLIN 0001, Core Labor AND/OR be similar to the efforts described below. To ensure maximum flexibility with respect to the CLIN 0002 Optional Labor, the contractor shall include a complete price list identifying the proposed hourly labor rates for all labor categories proposed to support CLIN 0001, Core Labor, for the life of the task order. Such rates will be used as the pricing basis to negotiate applicable firm fixed prices for the Optional Labor, when/if needed. The actual time frame for the CLIN 0002 Optional Labor support negotiation and implementation will be dependent upon actual scheduling requirements. Exercising the optional labor requirements will be incorporated via a bilateral agreement to the task order. During the course of the contract, the potential future requirements would be negotiated with the Contractor via a bilateral contract modification. In addition to increased support for CLIN 01, the below future requirements are representative of the potential support to be exercised under this CLIN:

- Development of new APIs or Web Services for integration with 3rd party systems
- Add new capabilities to DESKES, such as custom workflow process for routing approvals.
- Add Data analytics functionality for DDESB datasets

2.3 Other Direct Costs – CLIN 3

The Contractor is not authorized to incur any ODCs without the prior written approval of the COR on a DDESB Request for ODC Authorization form. There are three types of ODCs applicable under this order: Incidental Material, Travel, and Cloud Hosting Services. The contractor may not incur costs in excess of the funded value for either of these items.

- Material: Materials are those incidental items that are not included in the SOW but may be chargeable. However, materials shall not include items such as training, software

tools, and other materials needed by the Contractor to provide personnel under this Task Order.

- Travel: The Contractor must obtain advance written approval from the COR for all travel performed in connection with this Contract. Any travel expenses incurred, without prior written approval from the COR, will not be reimbursed by the Government. Travel expenses will be reimbursed based on the Joint Travel Regulations and the per diem rates established by the General Service Administration (meals and incidental expenses) in effect at the travel location, with lodging reimbursed at actual costs. Local travel under this Task Order is not authorized. Actual travel time incurred by the Contractor shall not be subject to reimbursement.

- Cloud Hosting Services: The DESKES version 6 will be hosted at the primary site, which will be Amazon Web Services (AWS) GovCloud (US) Region, a commercial Cloud Service Provider (CSP), located in the Northwestern region of the United States. A shared-responsibility model exists between DESKES and AWS through the Amazon Web Services General Support System Sensitive (AWS-GSS-S) – a cloud brokerage. This shared model can relieve projects' operational burden as AWS operates, manages, and controls the components from the host Operating System (OS) and virtualization layer down to the physical security of the facilities in which the services operate. The Contractor shall also provide cloud hosting services for the DESKES application suite. The contractor will also be responsible for supporting parts of DESKES located in Charleston, SC at the SPAWAR RDT&E lab. The hosting cost will be covered by the government at the SPAWAR facility.

  Contractor shall propose Service Level Agreements (SLA) with details relating to service availability and performance to include and note limited to:
  - uptime
  - service response time
  - problem response time and resolution time
  - data return

  The contractor shall propose provisions for the proposed Cloud solution data backups and storage, Disaster Recovery and Business Continuity plans in their proposal to DESKES.

3. Labor Requirements

The Contractor shall dedicate personnel who exhibit a professional history of implementing technical solutions and effectively communicating verbally and in writing, including the use of email, word processing, spreadsheet, and presentation tools. Technical writing skills, configuration management skills and quality assurance skills are necessary to support specific areas of the requirements in this PWS as is expertise with requirements development, management, design and implementation.

The Contractor shall identify personnel who have worked on custom software. The Offeror must have 100% of the proposed personnel with an active SECRET clearance by the beginning of the transition period of the task.

3.1. One hundred (100%) of contractor's personnel must maintain at least an Information Assurance Technician level II or Information Assurance Management level II (IAT or IAM Level II) certification or equivalent and all associate architects shall maintain at least an Information Assurance Technician level I or Information Assurance Management level I (IAT or IAM Level I) certification.

3.2. All contractor personnel supporting the tasks shall have experience working with Sharepoint integration with Java web application, and supported CORBA 2000 Web Service Architect.

3.3. Security Requirements

3.3.1. General Security Information. The majority of daily work associated with this PWS is at the unclassified level, but contractor personnel may be required to access SECRET areas, information and systems during the performance of this contract. The Contractor shall comply with DDESB administrative, physical, and technical security controls to ensure that all Government's security requirements are met. In addition, all Contractor personnel shall adhere to the DDESB's rules and regulations. The Contractor is responsible for addressing any issues or concerns raised by DDESB with five (5) workdays to resubmit revisions.

3.3.2. Citizenship and Clearance Requirements. The contractor's, subcontractors, and/or partner's personnel performing services under this task order shall be citizens of the United States of America. Overall, all contractor personnel shall possess the appropriate personnel security investigation for the position(s) occupied. Contractor personnel shall be required to have a background investigation that corresponds with the sensitivity level of the tasks to be performed.

3.3.3. Security Clearance and Special Access Requirements.

All positions on this task order require a minimum of a SECRET clearance as granted by the Personnel Security Management Office-Industry (PSMO-I).

3.3.4. Facilities Clearance (FCL)

The contractor must have a valid FCL at the SECRET level.

3.3.5. Personnel and Facilities Clearance Validation.

Upon award, the contractor shall submit the names of contractor personnel to the DDESB management, who is functional manager for this contract, for vetting through JPAS to ensure investigative and clearance requirements have been satisfied. This shall be completed before a request for issuance of the CAC to the contractor's personnel. If a contractor's employee does not have the required investigative or security clearance level based on the Government's determination, the contractor's employee will be denied the ability to work in support of DDESB.

3.3.6. Common Access Card Issuance Procedures.

Upon notification by DDESB management, the TA will create a CAC application in TASS with an expiration date of no more than three years. Contractors are reminded that once a new contract is issued, previously held Government CAC's or those from other contracts must be revoked, before a new CAC can be issued for the new contract. Once approved by the TA, the contractor employee may go to the nearest Real-Time Automated Personnel Identification System (RAPIDS)/Defense Enrollment Eligibility Reporting System (DEERS) office for CAC issuance.

4. Deliverables

Deliverables acceptance will be subject to Government acceptance testing to include required functionality and review of documentation. The Government will review and comment on all draft and deliverables within fifteen (15) working days of receipt, unless specified differently below. Acceptance or rejection of deliverables shall be made by the Contract Officer Representative (COR) in writing, giving the specific reason(s) for the rejection. The Contractor shall correct the rejected deliverable and return it on the date specified by the COR. While

deliverables are under review, Contractors will continue work on follow-on activities to maintain the project schedule.

Section	Deliverable Description	Delivery Schedule
2.1.1.1	Defect Documentation (Root Cause Analysis (RCA))	The initial report shall be delivered within twenty-four (24) hours of the initial report of the defect via email to the Government Program Manager and COR. Each report shall indicate the next estimated update. The Contractor shall make updates to the PM and COR following this schedule and/or when requested by the Government.
2.1.1.1	Location of Solution Software for Download Documentation	The Contractor shall provide documentation once per year 10 business days prior to the option year demonstrating where downloadable solution software and training material for external users accessing the system on non-Government Furnished Equipment is located and an updated list of solution software and training materials included.
2.1.2.1	Monthly Status Report (MSR)	Monthly by the 10th calendar of the month
2.1.2.3	Application Technical Roadmap	This Roadmap shall be reviewed and delivered twice each year to the Government PM and COR with at least six (6) months duration between each report.
2.1.2.2	Release & Performance Documentation	The Contractor shall be responsible to provide the following reports not to exceed the frequency indicated. The format shall follow Government mandated formats provided at the time of the request: System Security Plan Annual or as-required Program Management Plan Twice Annually Annual Continuity Plan project plan and training Annually US-Cert Incident Reporting Exercise Annually System Configuration (as-built) As Required

		Alternative Analysis for technical solutions (including estimates) As Required Training Materials As Required for new features or helpdesk findings
5.1	Phase In Plan	Phase In Transition Plan (draft) Due in Quote Phase In Transition Plan (final) 3 Days after COR comments are provided to Contractor
5.2	Phase Out Plan	Phase Out Transition Plan 60 calendar days prior to contract completion or termination

The Contractor shall deliver the deliverables specified in Section 5 (and any additional deliverables that the Contracting Officer may require in writing) on dates specified therein, or on such revised dates as the Contracting Officer may specify. . The Contractor may mark the deliverables to indicate its authorship, provided, however, that it shall not include any markings inconsistent with the Government unlimited rights. The Contractor agrees that the Government may release any deliverable in response to a Freedom of Information Act (FOIA) request, subject to any right to object or to request redactions that the Contractor may otherwise have under the Act or under applicable agency regulations.

All deliverables in printed or other media forms containing personally identifiable information (PII) and/or sensitive but unclassified (SBU) information shall follow applicable policies including DDESB Document security for Sensitive But Unclassified. The Contractor shall ensure and deliver the application is designed to function in accordance with applicable Federal Information Processing Standards Publication (FIPS PUB) 140-2 and all applicable annexes or subsequently approved federally recognized policy for the protection, operation and/or delivery of Federal information technology systems.

4.1 Government Review

Government personnel will have 15 business days to review deliverables (to include resubmissions) and provide written acceptance/rejection. Government representatives and/or the applicable Contracting Officer Representatives (CORs) will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 15 days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

4.2 Deliverable Rights

All information such as software, data, designs, test materials, documents, documentation, notes, records, software tools acquired, and/or software source code and modifications produced by the contractor under this PWS shall become the sole property of the U.S. Government, which shall have unlimited rights to all materials and determine the scope of publication and distribution. The contractor shall be required to deliver electronic copies of all documents, notes, records and software to the Government upon termination or expiration of the contract. The Government shall retain ownership of all proprietary information and intellectual property generated under this contract.

4.3Transfer of Ownership

All data and documentation, including all studies, reports, spreadsheets, software, data, designs, presentations, documentation, etc., produced by the contractor for the Government using this PWS are the property of the Government upon its taking possession of task deliverables or upon termination or expiration of the contract.

4.4 Monthly Invoice

- The contractor shall provide a monthly invoice, no later than the 15th calendar day of the month following the monthly reporting period, to be submitted simultaneously with the monthly status report. Both documents shall be provided to applicable parties. The invoice shall include but not be limited to:
- Clear identification of all costs.
- Travel costs.
- Supporting documentation for travel costs. Invoices including travel costs shall include supporting documentation as required by the Federal Travel Regulation (FTR) (receipts for all costs $75.00 or greater). Invoice submissions including travel costs shall include completed travel expense sheets (i.e. travel voucher) for each trip for each employee. All travel costs shall be compiled into the Government provided travel expense sheet (Attachment C). The travel expense sheet shall be submitted with the invoice.
- The contractor shall comply with line item (i.e., per individual positions, different programs, program areas, etc.) billing requests.

5. Place and Period of Performance

Work is expected to be performed from the contractor's work location, Mark Center, or virtually within the United States. Core hours will generally be 7:30 AM through 5:00 PM Eastern Time, Monday through Friday, excluding Federal holidays. One position shall be located on-site at the Mark Center. Other contract personnel work locations shall be within a 75 miles radius of the Mark Center.

The Period of Performance (PoP) will be one (1) base year (inclusive of a 30-day transition period (February 22, 2019 – February 21, 2024)) and four (w) option years, each with a duration of twelve (12) months. The anticipated period of performance will be February 22, 2019 through February 21, 2024.

Base Year	February 22, 2019 – February 21, 2020
Option Period 1	February 22, 2020 – February 21, 2021
Option Period 2	February 22, 2021 – February 21, 2022
Option Period 3	February 22, 2022 - February 21, 2023
Option Period 4	February 22, 2023 - February 21, 2024

Telework. Telework/telecommuting/contractor site is the primary method of accomplishing the work effort under this PWS with occasional site-based work on an as required basis. One FTE will be required to work onsite at Mark Center and all others within 75 miles.

Contractor shall develop telework policies to comply with the following requirements and address at a generic level within their Quality Control Plan. Alternate work arrangements for contractors shall be negotiated with the contractor's own employer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the contractor's responsibility to ensure the services are performed in accordance with the terms and conditions of the award. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities. The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities.
- Protecting information systems not under the control of the agency that are used for teleworking.
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking.
- Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

Phase-In/Phase-Out Overview
The Phase-In/Phase-Out process is defined as a smooth transition from one Contractor to another, in order to maintain the program's integrity required under this and the previous agreements.

The Contractor shall take all actions necessary to achieve a successful transition from the incumbent Contractor to the follow-on Contractor.

5.1. Phase-In

The incumbent contractor shall be prepared to provide all source code documentation to the incoming contractor on the first day of the phase-in period. The Contractor shall develop a draft Phase-In Plan detailing the phase-in approach, staffing, activities, risks, and schedule as part of their quote to ensure business continuity with no disruption and no impact to existing systems. After award, the COR will provide the Contractor feedback on the phase-in plan and allow the Contractor to make revisions as needed. The Contractor shall resubmit the Final Phase-In Plan three (3) business days after COR provides feedback to the Contractor. The Contractor shall follow the Government approved phase-in transition plan. The Contractor shall propose a transition timeline and process for any phase-in activities as required. The Contractor shall expect to attend an orientation session at or before the start of the award. This session may be virtual or at a central location.

The Contractor shall prepare for and achieve full operational status on the first week of the phase-in of the phase in. This is to ensure enough time is given to understanding the unique custom application. Site access shall be permitted during phase-in to the extent that it does not interfere with the operation of the Incumbent Contractor. The Contractor shall coordinate with the COR for site access permission.

Though the contract's anticipated period of performance begins on February 22, 2019, though some requirements/tasks may require a Phase-In Process. The Phase-In Process shall be limited to February 22, 2019 to March 24, 2019 or as specified through the CO. One Hundred (100%) percent of all contractor staff shall have required DDESB clearances at the start of the Phase in Period.

The Contractor shall ensure the DESKES application is operational and fully functional with no performance or access degradation on the date the contractor assumes responsibility for DESKES O&M.

5.2.Phase-Out

The Contractor shall maintain fully operational during the period of time leading up to the contract's expiration or termination. The Contractor shall submit to the Government a phase-out plan sixty (60) calendar days before the contract's completion or termination. The Phase Out period shall begin 30 days prior the contract's completion or termination. The DESKES environment shall be immediately transferable to DDESB or DDESB's designee upon completion of this task.

The phase-out plan shall address not less than the following.

- Procedures for retaining the staffing levels necessary to maintain required services through the day of the contract's expiration or termination.
- Procedure and responsibilities for performing physical inventory and reconciliation of Government Furnished Equipment (GFE) and Government Furnished Information (GFI).
- Procedure and responsibility for reconciling and certifying material and equipment on-hand levels and accuracy.

- Document and define the procedures and responsibilities for turning over all account access to the follow-on contractor required to manage and maintain the cloud environment.
- Document and define the plan for providing on-the-job, application specific, training for the incoming Contractor personnel
- Provide detailed documentation sufficient to allow follow-on Contractor to effectively transition into the contract. The following illustrates the type of documentation required. The Government will specify any other types of documentation that may be needed at the start of the phase-out period.
    - System operating procedures
    - Detailed data mapping
    - All business logic and where it resides within the system (presentation layer, database, etc.)
    - All workflows and business processes
    - All outstanding / in-progress issues
    - All undeveloped requirements
    - Latest version of the System Security Plan
    - Any additional documents developed related to the system.
- The Contractor shall provide application and code walkthroughs with the incoming vendor.
- The Contractor shall provide the code repository/ code base.
- The Contractor shall provide the hardware and software inventory.
- The Contractor shall facilitate the transition of the cloud environment to incoming vendor and/or DDESB, as DDESB's determines.
- The Contractor at the end of the contract Phase Out period shall turn over the DESKES cloud environment to the incoming vendor or DDESB at DDESB's discretion including the transfer of all related Service Accounts.
- The Contractor shall provide continuing O&M / facilitating transition until final cutover to incoming vendor, at which point a transfer of service accounts would coincide with the transfer of responsibility.
- The Contractor shall coordinate its phase-out activities with the incoming Contractor to effect a smooth and orderly transition at the end of the contract period.
- The Contractor shall provide on-the-job, application-specific, training for the incoming Contractor personnel, as needed.
- The Contractor shall schedule and facilitate shadowing activities with the incoming vendor.
- The Contractor shall provide written Question and Answer sessions with the incoming vendor. Responses to all questions will be documented.

The Contractor shall coordinate its phase-out activities with the incoming Contractor/Government personnel to affect a smooth and orderly transition at the end of the contract's period of performance. The Contractor shall provide on-the-job training for the incoming Contractor personnel, as needed by the in-coming Contractor, except for IT training. The Contractor shall remove all Contractor-owned property from the Government space or facility by close of business on the last day of the contract.

6. Travel

Travel must be coordinated and authorized by the Contracting Officer or the Contracting Officer Representative prior to incurring costs. Contractor costs for travel will be reimbursed in accordance with FAR 31.205-46, in arrears. The travel costs shall be reasonable and allowable as defined in FAR 31.201 and in accordance with the limitations of the JTR.

The contractor shall invoice monthly on the basis of cost incurred. The contractor must provide documentation in support of all travel expenses. The contactor will not be reimbursed for local travel (within a 50-mile radius of the Government/contractor's facility) or commuter travel (commute from home to work site).

Invoice submissions including travel costs shall include completed travel expense sheets (i.e., travel voucher) for each trip and each employee who traveled. The travel expense report, receipts of $75 or more (with exceptions being lodging and transportation), and supporting documentation (e.g., approval email for exceeding per diem rates, cost comparisons, etc.) shall be submitted with the invoice. Expense report(s) must include the traveler's name, dates of travel, destination, purpose of travel, Approval Authority documentation (e.g., copy of the e-mail authorizing travel by Government official), and cost for each trip. All travel costs shall be compiled into the Government provided travel expense sheet (PWS Addendum 1) or similar document that has been determined to be acceptable by the Government. The entire submission shall be complete and organized to enable the Government to complete an efficient review. Submissions that are not complete and organized are subject to rejection.

Local travel is not reimbursable. Local travel shall be considered within fifty (50) miles from Mark Center.

7. Government Furnished Equipment (GFE)/ Government Furnished Information (GFI)

Government Furnished Equipment (GFE) or Government Furnished Information (GFI) will be provided to the Contractor during the period of performance of the contract, under the following conditions:

a. Use of the GFE and GFI is for the sole purpose of completing the requirements of this contract
b. The contract employee has already received a final SECRET determination/adjudication.

Note: GFE may include virtual desktop access provided by DDESB and does not necessarily constitute the distribution of laptops to the Contractor. Access to the JSP network, whether direct or through other means, such as the JSP Virtual Private Network (VPN), is contingent upon each contract employee having Active SECRET.

The estimated GFE is three DDESB issued laptops as determined by the Government.

The anticipated GFI shall include but is not limited to all work, work products, and documentation related the design, development, implementation and management of the DESKES AWS or other DESKES cloud instance. DDESB owns all elements related to the DESKES AWS or other cloud instance exclusive of the infrastructure and services provided by AWS or other cloud provider. At the conclusion of the contract, all access required to manage the ePM cloud environment such as Service Accounts will be turned over at DDESB's discretion to DDESB or another vendor.